

WHAT IS CLAIMED IS:

1. A computer-readable medium having computer-executable instructions, comprising:

receiving a first transaction request in association with
5 a first certificate issued by a certificate authority;

communicating with a status authority to query for
current status information on the first certificate; and

receiving a second certificate from the status authority
indicating the current status of the first certificate.

10

2. The computer-readable medium of claim 1, wherein the
certificate authority comprises the status authority.

3. The computer-readable medium of claim 1, wherein the
15 status authority comprises an agent authorized to act on
behalf of the certificate authority.

4. The computer-readable medium of claim 1, wherein the
transaction request is received from an end entity, and having
20 further computer executable instructions comprising,
transmitting information including the second certificate to
the end entity.

a1 5 5. The computer-readable medium of claim 4, wherein the information including the second certificate is transmitted to the end entity along with a response to the transaction request.

6. The computer-readable medium of claim 4, wherein the information including the second certificate is transmitted to the end entity along with at least one digital signature.

10 7. The computer-readable medium of claim 1 having further computer executable instructions comprising, transmitting the first certificate and the second certificate to a remote party along with a second transaction request.

15 8. The computer-readable medium of claim 7 having further computer executable instructions comprising, receiving a third certificate from the remote party.

20 9. The computer-readable medium of claim 8, wherein information of the third certificate is communicated with a response to the second transaction.

10. The computer-readable medium of claim 1, wherein a third certificate is received with the transaction request and

the first certificate, the third certificate comprising a record of a response to a status request of the first certificate at a particular time.

5 11. The computer-readable medium of claim 10 having further computer executable instructions comprising, transmitting the first certificate, the second certificate, and the third certificate to a remote party along with another transaction request.

10 12. The computer-readable medium of claim 11 having further computer executable instructions comprising, receiving information including a fourth certificate from the remote party indicating the current status of at least one of the
15 first, second, and third certificates.

20 13. The computer-readable medium of claim 11, wherein the fourth certificate is communicated with a response to the other transaction.

14. A computer-readable medium having computer-executable instructions, comprising:

receiving a query from a relying party for current status information on a first certificate; and

a
issuing a data structure including a second certificate
indicating the current status of the first certificate.

15. The computer-readable medium of claim 14, having
5 further computer executable instructions comprising
transmitting the data structure to the relying party.

16. The computer-readable medium of claim 14, wherein
the data structure comprises an extension designating the
10 second certificate as being an indication of the current
status of the first certificate.

17. The computer-readable medium of claim 14, wherein
the data structure further comprises policy information.
15

18. The computer-readable medium of claim 17, wherein
the data structure further includes information regarding
evidence submitted to satisfy a policy of the relying party.

20 19. The computer-readable medium of claim 14, wherein
the data structure comprises policy-related information that
qualifies the second certificate.

20. The computer-readable medium of claim 14, wherein the data structure further comprises success or failure information regarding the second certificate.

5 21. The computer-readable medium of claim 14, wherein the data structure comprises information regarding a validity period of the second certificate.

10 22. The computer-readable medium of claim 21, wherein the first certificate has a validity period associated therewith, and wherein the information regarding the validity period of the second certificate specifies a validity period for the second certificate that is shorter than the validity period for the first certificate.

15 23. A method for performing electronic commerce, comprising,

receiving, at a certificate authority, a first request for a certificate;

20 verifying whether the certificate should be issued, and if so, issuing the certificate;

receiving a second request at a status authority for status information about the certificate; and

issuing a reissue certificate including the status information.

24. The method of claim 23 wherein the certificate
5 authority comprises the status authority.

25. The method of claim 23 wherein the status authority
is a designated agent of the certificate authority.

26. The method of claim 23 wherein the first request is
10 provided by an end entity.

27. The method of claim 23 wherein the second request is
provided by a relying party.

28. The method of claim 23 wherein the first request is
provided by an end entity that provides the certificate to a
relying party, and wherein the second request is provided by
the relying party.

29. A method for performing electronic commerce,
20 comprising:

receiving a certificate at an end entity;
providing the certificate to a relying party; and

receiving a receipt at the end entity from the relying party, the receipt including status information about the certificate.

5 30. The method of claim 29 further comprising,
requesting the certificate from a certificate authority.

31. The method of claim 29 wherein the status information is provided by a status authority.

10 32. The method of claim 29 further comprising,
requesting a certificate from a certificate authority, and
wherein the status information is provided by the certificate authority.

15 33. The method of claim 29 wherein the receipt includes evidence.

20 34. The method of claim 33 wherein the evidence comprises policy information.

35. A method for performing electronic commerce, comprising,

receiving a certificate with a request to perform a transaction;

communicating with a status authority to request status information about the certificate;

5 receiving a reissue certificate including the status information in response to the request; and

deciding whether to perform the transaction based on the status information.

10 36. The method of claim 35 wherein the certificate is issued by a certificate authority.

37. The method of claim 35 wherein the certificate authority further comprises the status authority such that the
15 certificate and reissue certificate are issued by the certificate authority.

38. The method of claim 35 wherein the request to perform a transaction is received from an end entity, and
20 further comprising returning a response to the end entity.

39. The method of claim 35 wherein the response includes a receipt.

40. The method of claim 35 wherein the receipt includes data associated with the status information.

a 5 41. The method of claim 35 wherein the certificate is issued by a certificate authority, and wherein the request to perform a transaction is received from an end entity, and further comprising returning a response to the end entity.

10 42. A method for performing electronic commerce, comprising:
requesting at an end entity a certificate from a certificate authority;
providing the certificate with a request for performance of a transaction; and
15 receiving information at the end entity indicating whether the transaction was performed, the information provided by a status authority and including the status of the certificate.

20 43. The method of claim 42 wherein the certificate authority comprises the status authority.

44. The method of claim 42 wherein the information received at the end entity includes a receipt.

45. A method for performing electronic commerce,
comprising:

a 5 requesting at an end entity a certificate from a
certificate authority;

providing a request for performance of a transaction to a
relying party, the request including the certificate;

10 receiving the request at the relying party, and
communicating with a status authority to determine the status
of the certificate;

receiving a reissue certificate from the status
authority, the reissue certificate indicating the status of
the certificate; and

15 communicating information from the relying party to the
end entity, the information indicating whether the transaction
was performed and including the status of the certificate.

46. A method for performing electronic commerce,
comprising:

20 receiving, at a second party, a request from a first
party to accept a transaction and a first certificate
referencing the transaction;

accepting the transaction at the second party and issuing a receipt to the first party, the receipt including a second certificate as proof of acceptance of the transaction;

5 sending, from the second party to a third party, the transaction, the first certificate and the second certificate to offer the transaction for sale; and

receiving a receipt at the second party from the third party including a third certificate as proof that the third party purchased the transaction.

10 47. The method of claim 46 wherein the third party sends the transaction, the first certificate, the second certificate and the third certificate to a fourth party to attempt to resell the transaction.

15 48. The method of claim 46 wherein the fourth party purchases the transaction and issues a receipt including a fourth certificate to the third party.

20 4948. The method of claim 46 wherein the first certificate comprises evidence, and wherein the second party evaluates the evidence from the first party.

50 49. The method of claim ⁴⁹~~48~~ wherein the evidence includes
at least one policy decision made by the first party.

a 5 51~~50~~. The method of claim 46 wherein the first and second
certificates comprise evidence, and wherein the third party
evaluates the evidence from the first party and the second
party.

10 52 51. The method of claim ⁵¹~~50~~ wherein the evidence includes
at least one policy decision made by at least one of the first
or second parties.

15 53 ~~52~~. The method of claim 46 wherein the first, second and
third certificates comprise evidence, and wherein the fourth
party evaluates the evidence from the first party, the second
party and the third party.

20 54 ~~53~~. The method of claim ⁵¹~~50~~ wherein the evidence includes
at least one policy decision made by at least one of the
first, second or third parties.

55 ~~54~~. The method of claim 46 wherein each party evaluates
each certificate provided thereto prior to issuing its
respective receipt.

56 55. A computer-readable medium having stored thereon a data structure, comprising:

a first field referencing a request for performing an electronic transaction; and

a second field comprising a list of evidence accumulated from at least one recipient of the request.

57 56. The computer-readable medium having stored thereon the data structure of claim 56, wherein the first field comprises a response subject field.

58 56. The computer-readable medium having stored thereon the data structure of claim 56 further comprising, a third field having response status information therein.

59 56. The computer-readable medium having stored thereon the data structure of claim 56 further comprising, a third field having response status information therein.

60 56. The computer-readable medium having stored thereon the data structure of claim 56 further comprising, a third field having a validity period identified therein.

6160. The computer-readable medium having stored thereon the data structure of claim ⁵⁶~~55~~ further comprising, a third field having certificate policy information therein.

a 5 6261. The computer-readable medium having stored thereon the data structure of claim ⁵⁶~~55~~ further comprising, a third field having certificate policy information therein.

6362. A computer-readable medium having stored thereon a data structure, comprising,
a first data field representing the current status of a first certificate; and
a second data field designating the present data structure as including status information regarding the first certificate.

6463. The computer-readable medium of claim ⁶³~~62~~, wherein the data structure further comprises a third data field providing an evidence list.

20 6564. The computer-readable medium of claim ⁶³~~62~~, wherein the data structure further comprises information regarding evidence submitted to satisfy a policy of the remote recipient.

a¹ ~~66~~⁶³ 65. The computer-readable medium of claim ~~62~~⁶³, wherein the data structure comprises policy-related information.

5 ~~67~~⁶³ 66. The computer-readable medium of claim ~~62~~⁶³, wherein the current status field indicates success or failure information.

10 ~~68~~⁶³ 67. The computer-readable medium of claim ~~62~~⁶³, wherein the data structure comprises information regarding a validity period.